WHISTLEBLOWING-POLICY

thinkproject

Management system: Compliance
ALL
Document ID: CMS_0004
Version: 1.1
Classification: Open

Created by	Peter Mezger	15.07.2022
Approved by	Markus Scheuermann	15.07.2022
Date of original issue	29.07.2021	

Please do not print copies of this document.

CONTENT TABLE

1 SUMMARY

The thinkproject whistleblower system is intended to enable employees and other persons to submit anonymous reports. The whistleblower system is intended to record such reports in an easily comprehensible process that ensures the best possible protection of the legitimate interests of those involved. The whistleblower system aims to prevent both financial damage to the company and a loss of image.

Whistleblowing is only intended for the following categories of violations of rules set are / maybe relevant or close to criminal law:

- Conflicts of interest,
- corruption and bribery,
- public contract law,
- financial services, financial products, and financial markets,
- prevention of money laundering and terrorism funding,
- product safety and compliance,
- environmental protection,
- food and animal nutrition safety,
- health,
- protection of privacy and personal data
- network and information systems security
- competition law
- the 10 principles of the United Nations Global Compact

This whistleblower policy is also intended to ensure, from a technical and organizational perspective, that reports of violations of laws, the Code of Conduct, or guidelines are received according to the Code of Conduct requirements and data privacy and data security. And that they are processed, stored, and archived with the necessary confidentiality.

If local regulations are stricter than the minimum standards laid down in this directive minimum standards, the more stringent rules shall apply in each case. If there is a conflict between relevant laws and this policy, the affected party shall inform the Chief Compliance Officer to resolve the conflict.

2 SCOPE

This policy applies to all executive officers, directors, employees, contracted and temporary workers in all locations worldwide and to all Company representatives, including consultants and agents.

3 POLICY CONTENTS

OBLIGATION TO REPORT

Any employee and other persons of the thinkproject group are entitled to submit reports. It is irrelevant whether they are employees of a thinkproject group company or a subsidiary of a thinkproject group company.

To the extent permitted by law and to the extent consistent with conducting an adequate investigation, the company will protect the confidentiality and anonymity of the person making the report.

This policy does not imply any requirement for anyone to report. However, if there are legal, contractual, or other duties or obligations to provide reports, these are not affected by the above paragraph.

NO ACT OF RETALIATION

Employees and others who report will not be harassed, retaliated against, or suffer adverse employment consequences, such as discharge, demotion, suspension, discrimination with respect to the terms and conditions of employment. However, employees and associated persons who retaliate against an individual who has reported an incident in good faith will be subject to disciplinary action, up to and including termination.

SUBMISSION OF REPORTS

The submission of reports of actual or suspected violations shall be made possible as described below:

- Reports can be reported confidentially to the direct supervisor;
- Reports can be reported directly and confidentially to the compliance department;
- Reports can be reported directly via the digital whistleblower system.

In the digital whistleblower system, the forms of reports are technically predefined. In all other cases, however, the submission of reports is not bound to a specific format. An up-to-date overview of the reporting channels can be found at: https://thinkproject.integrityline.com/

RELEVANT REPORTS

The whistleblower system is provided solely to receive, and process reports of any alleged or actual violations of laws, policies, or the Code of Conduct. It is not available for general complaints or product and warranty inquiries.

Only those reports should be submitted where the whistleblower believes in good faith that the information provided by him/her is correct. On the other hand, the person is not in good faith if he/she knows that a reported fact is untrue. In case of doubt, corresponding facts are not presented as a fact but as an assumption, evaluation, or statement of other persons.

It is noted that a whistleblower may be liable to prosecution if, against his or her better knowledge, he or she alleges untrue facts about other persons.

PROTECTION OF THE WHISTLEBLOWER

All reports, including references to the whistleblower, will be processed confidentially and in accordance with applicable laws.

LEGAL RESTRICTIONS

The laws in some countries prescribe certain restrictions for reports, e.g., what may be reported, whether personal data about an individual may be stored, or whether reports can be made anonymously. The corresponding requirements are integrated into the digital whistleblower system. Any concerns that cannot be reported using the mentioned reporting procedures due to such restrictions should be directed to the employee's supervisor. If an employee feels that it is not possible to raise the matter locally, they should escalate it within the business unit to the local HR representative or the compliance department.

4 CONFIDENTIALITY AND DATA PROTECTION

All reports, regardless of their truthfulness, are likely to damage the reputation of the persons concerned, the whistleblowers and/or third parties, and the company.
We, therefore, treat them with confidentiality, over and above the obligations arising from the data protection laws. In addition to the register of data processors, which must always be kept up to date, a written record must be kept of the persons who may work with related data and what rights they have in the context of data processing. These persons must be obligated to observe special confidentiality over and above any legal requirements.

5 IT AND DATA SECURITY

IT solutions for the intake and processing of reports must be approved by the Information Security Officer, the Compliance Officer, and the Group Data Protection Officer before they are used. The minimum requirements for the scope of the General Data Protection Regulation are derived from Art. 32 of the GDPR, the Group guidelines on IT security and data protection. The sensitivity of the information and the risks to persons and the company if data relating to the information becomes known must be considered appropriately. The efficient and effective processing of reports is guaranteed and strictest confidentiality, particularly the employee's anonymity, for reports of any kind.

6 DELETION OF DATA

The deletion of data in the digital whistleblower system must be carried out exclusively in accordance with the respective time specifications of the deletion concept or after deletion approval by two separate users (four-eyes principle).

7 DOCUMENT CONTROL

Version	Date	Author	Approved by	Details of changes made
001	17.06.21	Peter Mezger	Ralf Grüßhaber	First version

1.1	15.07.22	Peter Mezger	Markus Scheuermann	Expansion Section 1